

We claim:

1 1. A cross-domain authentication apparatus, the apparatus comprising:
2 a first computer and a second computer;
3 a network connecting the first and second computers;
4 a secret shared between the first and second computers; and
5 a federation access policy identifying access permission on the first computer for a
6 user local to the second computer over the network.

1 2. An apparatus according to claim 1, the apparatus further comprising an HTTP
2 reverse proxy coupled to the first computer, the proxy designed to request an authentication
3 challenge of the user from the second computer.

1 3. An apparatus according to claim 2, the apparatus further comprising an HTTP
2 forward proxy coupled to the second computer designed to respond to the authentication
3 challenge for the user and forward the authentication to the reverse proxy.

1 4. An apparatus according to claim 3, wherein the response to the authentication
2 challenge includes an encrypted response keyed to the shared secret.

1 5. An apparatus according to claim 1, the apparatus further comprising a security
2 module designed to implement the federation access policy.

1 6. An apparatus according to claim 1, wherein:
2 the federation access policy includes an access for a role identity; and
3 the apparatus further comprises an identity mapping from the user to the role identity.

1 7. An apparatus according to claim 6, wherein the identity mapping is designed
2 to enable access to a resource on the first computer across different formats and encodings of
3 user names.

1 8. An apparatus according to claim 1, the apparatus further comprising an access
2 control entry in the federation access policy designed to enable access to a resource on the
3 first computer by a user on the second computer.

1 9. An apparatus according to claim 8, wherein the federation access policy is
2 designed to permit a second user on the first computer to define the access control entry
3 without requiring assistance from an administrator.

1 10. An apparatus according to claim 9, wherein the access control entry includes a
2 permission for the user on the second computer that is equal to or less than a permission
3 available to the second user on the first computer.

1 11. An apparatus according to claim 8, wherein the access control entry refers to a
2 public key certificate for the user on the second computer whose access is controlled by the
3 access control entry.

1 12. An apparatus according to claim 11, wherein the apparatus further comprises
2 means for automatically retrieving from the second computer the public key certificate for the
3 user on the second computer without human intervention.

1 13. An apparatus according to claim 12, wherein the means for automatically
2 retrieving includes a background mutual authenticator operable through a Secure Sockets
3 Layer (SSL) protocol.

1 14. An apparatus according to claim 8, wherein the federation access policy is
2 designed to permit a second user on the first computer to remove or modify the access control
3 entry, the second user having a privilege to remove or modify the access control entry.

1 15. An apparatus according to claim 14, wherein the second user is the user who
2 defined the access control entry.

1 16. An apparatus according to claim 8, wherein the access control entry is
2 designed to enable access to the resource on the first computer across different formats and
3 encodings of user names.

1 17. An apparatus according to claim 1, wherein the federation access policy
2 includes a resource to which the user is permitted access.

1 18. An apparatus according to claim 1, the apparatus further comprising a
2 temporary data file indicating that the user has been properly authenticated.

1 19. A method for performing cross domain authentication, the method comprising:
2 receiving a request for a resource on a first computer from a user local to a second
3 computer over a network;
4 challenging the user to be authenticated;
5 authenticating the user;
6 informing the first computer that the user is authenticated; and
7 accessing the resource from the first computer using the second computer.

1 20. A method according to claim 19, wherein authenticating the user includes
2 authenticating the user at the second computer.

1 21. A method according to claim 20, wherein informing the first computer
2 includes returning the authentication to the first computer.

1 22. A method according to claim 19, wherein receiving a request includes:
2 receiving the request at a forward proxy coupled to the second computer; and
3 forwarding the request to a reverse proxy on the first computer.

1 23. A method according to claim 19, wherein receiving a request includes
2 requesting the resource by the user from the second computer.

1 24. A method according to claim 19, wherein challenging the user includes
2 sending a challenge authentication from the first computer to the second computer.

1 25. A method according to claim 24, wherein sending a challenge authentication
2 includes sending a challenge authentication from a reverse proxy at the first computer to a
3 forward proxy at the second computer.

1 26. A method according to claim 24, wherein sending a challenge authentication
2 from a reverse proxy includes redirecting the user to a mediator coupled to a forward proxy at
3 the second computer.

1 27. A method according to claim 26, wherein authenticating the user includes
2 authenticating the user using the mediator.

1 28. A method according to claim 27, wherein authenticating the user further
2 includes sending from the forward proxy a keyed hash response to the challenge
3 authentication using a shared secret between the first computer and second computer.

1 29. A method according to claim 19, the method further comprising negotiating a
2 session secret key needed for encrypting or integrity protecting the response to the access
3 request.

1 30. A method according to claim 29, wherein accessing the resource includes
2 encrypting a response using the negotiated session secret key.

1 31. A method according to claim 30, wherein encrypting a response includes
2 encrypting the response using the session secret key at a reverse proxy of the first computer
3 before sending the response to a forward proxy of the second computer over the network.

1 32. A method according to claim 30, wherein accessing the resource includes
2 decrypting the response at a forward proxy of the second computer before sending the
3 response to the user at the second computer.

1 33. A method according to claim 29, wherein accessing the resource includes
2 integrity-protecting a response using the session secret key.

1 34. A method according to claim 33, wherein integrity-protecting a response
2 includes integrity-protecting the response using the session secret key at a reverse proxy of
3 the first computer before sending the response to a forward proxy of the second computer
4 over the network.

1 35. A method according to claim 33, wherein accessing the resource includes
2 integrity-verifying the response at a forward proxy of the second computer before sending the
3 response to the user at the second computer.

1 36. A method according to claim 19, wherein accessing the resource includes
2 accessing the resource from the first computer over the network.

1 37. A method according to claim 19, wherein accessing the resource includes
2 determining whether the user has permission to access the resource.

1 38. A method according to claim 37, wherein determining whether the user has
2 permission includes checking a federation access policy to determine whether the user has
3 permission to access the resource.

1 39. A method according to claim 38, wherein checking a federation access policy
2 includes:
3 using an identity mapping in the federation access policy to map the user to a local
4 identity; and
5 checking that the local identity is permitted to access the resource.

1 40. A method according to claim 39, wherein using an identity mapping includes
2 using the identity mapping in the federation access policy to map the user to the local
3 identity, allowing for different formats and encodings of user names between the first and
4 second computers.

1 41. A method according to claim 38, wherein checking a federation access policy
2 includes using an access control entry in the federation access policy to determine if the user
3 is permitted to access the resource.

1 42. A method according to claim 41, wherein using an access control entry
2 includes using the access control entry in the federation access policy to determine if the user
3 is permitted to access the resource, allowing for different formats and encodings between the
4 first and second computers.

1 43. A method according to claim 19, wherein authenticating the user includes
2 authenticating the user using a third party as a mediator.

1 44. A method according to claim 43, wherein accessing the resource with the
2 second computer includes maintaining channel integrity between the first computer and the
3 second computer over the network.

1 45. A method according to claim 19, wherein decrypting or integrity verifying the
2 access response at the forward proxy of the second computer network is done before the
3 response is sent to user at the second computer network.

1 46. A computer-readable medium containing a program to perform cross domain
2 authentication on a computer system, the program being executable on the computer system
3 to implement the method of claim 19.